

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

PATENT

RECEIVED
CENTRAL FAX CENTER
FEB 09 2011

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Inventors: Gervais, John Alan, et. al.

Serial No: 10/582,676

Group Art Unit: 2492

Filed: June 12, 2006

Docket: PU030342

For: SECURE PORTING OF INFORMATION FROM ONE DEVICE TO ANOTHER

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Applicants appeal the status of Claims 1-9 as rejected in the final Office Action dated June 22, 2010 and the Advisory Action dated October 19, 2010, pursuant to the Notice of Appeal filed November 22, 2010 and submit this appeal brief.

02/10/2011 MMARZII 00000008 070832 10582676

01 FC:1402 540.00 DA

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being faxed to the United States Patent & Trademark Office, fax # 571-273-8300, Mail Stop: Appeal Brief-Patents on:

Date

2-9-11

Fideliz Romero

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

TABLE OF CONTENTS:

1.	Real Party in Interest	Page 3
2.	Related Appeals and Interferences	Page 4
3.	Status of Claims	Page 5
4.	Status of Amendments	Page 6
5.	Summary of Claimed Subject Matter	Page 7
6.	Grounds of Rejection to be Reviewed on Appeal	Page 11
7.	Argument	Page 12
8.	CLAIMS APPENDIX	Page 25
9.	RELATED EVIDENCE APPENDIX	Page 32
10.	RELATED PROCEEDINGS APPENDIX	Page 33

PATENT

Custmer No. 24498

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

1. Real Party in Interest

The real party in interest is THOMSON LICENSING S.A., the assignee of the entire right title and interest in and to the subject application by virtue of assignments recorded with the Patent Office on June 12, 2006 at reel/frames 018208/0678; on June 12, 2006 at reel/frames 018208/0697; and on April 27, 2007 at reel/frames 019231/0351.

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

PATENT

2. Related Appeals and Interferences

Appellant is not aware of any appeals or interferences related to the present application.

PATENT

Customer No. 24498

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

3. Status of Claims

- a) Claims 1–13 are pending. Claims 1, 6, 8, 9, 10 and 13 are independent.
- b) Claims 10 – 13 have been allowed.
- c) Claims 1–9 stand rejected and are under appeal.

Custmer No. 24498

PATENT

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

4. Status of Amendments

No amendments were made in the response to the Final Office Action of June 22, 2010. As such, the claims stand as previously presented.

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

5. Summary of Claimed Subject Matter¹

Independent Claim 1 is directed to a device comprising:

a removable digital memory including a port at which digital information stored on said removable digital memory can be accessed (p. 4, lns 5 – 13, and FIGS. 1 – 5, block 18, 18IO);

a memory for storing first conditional access data and at least one content encryption key (p. 4, lns 18 – 21, p. 7, lns 6 – 10, and FIGS. 1 – 2, block 16, FIGS. 3 – 4, block 16, 318);

a second port for receiving user certificate data and a first key of a key pair contained in a write once memory of an access card that has been paired with a destination device (p. 4, lns 18 – 21, p. 5, lns 15 – 20, p. 6, lns 14 – 29, and FIG. 3, block 22, 30, 40, 44, 46); and

a processor responsive to the user certificate data received on said second port for authenticating the received certificate data based on the first conditional access data stored in said memory, the processor, upon said authentication, encrypting information stored in said removable digital memory using the at least one content encryption key, to thereby provide encrypted information in said removable digital memory, the processor operable for encrypting said content encryption key using said first key received on said second port and outputting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device (p. 5, lns 29 – 33, p. 6, p. 7, lns 6 – 12, FIG. 2, block 210, 212, and FIG. 4, block 405).

¹ It should be explicitly noted that it is not the Appellant's intention that the currently claimed or described embodiments be limited to operation within the illustrative embodiments described below beyond what is required by the claim language. Further description of the illustrative embodiments are provided indicating portions of the claims which cover the illustrative embodiments merely for compliance with requirements of this appeal without intending to read any further interpreted limitations into the claims as

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

Independent claim 6 is directed to an access card for enabling secure accessing of digital information stored on a removable memory, the access card comprising:

a memory having stored therein a first conditional access certificate and a second conditional access certificate (p. 5, lns 15 – 25, and FIG. 1, block 40, 42, 44);

a write once memory (p. 6, lns 12 - 17 and FIG. 1, block 40);

means for authenticating first and second conditional access certificates with respective first and second certificate data stored on respective destination and source devices (p. 6, lns 4 – 9, p. 6, lns 33 – 37, and FIG. 2, block 210, 212, and FIG. 3, block 310) ;

said write once memory, following authentication of said card with a destination device, being updated to store a public key of a public/private key pair stored in said destination device to thereby pair the access card with said destination device (p. 6, lns 12 – 29, and FIG. 2, blocks 30, 40, 46, 36, 210, 212); and

a processor operable for, upon authentication of said card with a source device, controlling transmission of said public key to said source device, wherein, in response thereto, said memory being updated to store encrypted data comprising a first key encrypted using said public key, said first key also being used to encrypt information on said removable memory at said source device, whereby communication of said encrypted data to said destination device enables decryption of said data using said private key to recover said first key, to thereby decrypt encrypted information in said removable memory (p. 6 ln 30 – p. 7 ln 12, p. 7 lns 36 – p. 8 ln 6, FIG. 3, blocks 310, 312, FIG. 4, blocks 405, 406, FIG. 5, 510, 512).

presented

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

Independent claim 8 is directed to a digital information destination device comprising:

a digital information input port (p. 5, lns 3 – 6 and FIG. 1, 30 DATA);

a digital information decoder coupled to said digital information input port for decoding digital information encoded with a content encoding key, when said content encoding key is available, to thereby produce unencoded digital information (p. 7, lns 32 – p. 8 lns 6, p. 8, lns 16 – 19, and FIG. 5 blocks 30 DATA, 418, 540);

memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device (p. 4 lns 31 – 36 and FIG. 5, blocks 30, 32, 34, 36);

a content encoding key decryptor for decrypting said content encoding key with a content encoding key encryption key (p. 2 lns 39 – p.3 lns 3, FIG. 5, block 34);

an access card reader for reading an access card, where said access card includes authentication means and a write once memory which, prior to a first insertion in said destination device, includes at least a second Conditional Access Certificate and a first User Certificate and which, after said first insertion, includes at least said public portion of said private and public encryption keys thereby pairing the access card and the destination device and which, prior to a subsequent insertion in said destination device, is inserted into a source device and updated to include a content encoding key encrypted with said key encryption key, whereby said destination device, following said subsequent insertion of said access card, has the key encryption key and can decrypt said content encoding key and, using said content encoding key, decode said digital information encoded with said content encoding key (p. 1 ln 37 – p. 3 ln 5, FIG. 5, blocks 38, 42, 44, 46 440, 540).

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

Independent claim 9 is directed to a method for securely transferring information from a source device to an external device, the source device having a removable digital memory containing information accessible to the source device, the information contained in said digital memory intended to be protected from unauthorized access, the method comprising:

receiving at the source device user certificate data from an access device that has been paired with a destination device and comparing the user certificate data with a first Conditional Access Certificate stored in memory of said source device for authenticating the certificate data (p. 6, lns 30 – 38, and FIG. 3, blocks 12, 14, 16, 30, 40, 44);

accessing, by said source device, said information stored in said removable digital memory and encrypting said information stored in said removable digital memory using at least one content encryption key stored in said source device, upon authentication of said certificate data (p. 7, lns 6 – 10, and FIG. 4, blocks 405, 414);

receiving at the source device a public key from a write once memory of the access device and encrypting said at least one content encryption key using said public key (p. 6, lns 30 – 38, FIG. 4, blocks 405, 414); and

transmitting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device communicable with said access device (p. 7, lns 6 – 12, FIG. 5, block 510).

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

6. Grounds of Rejection to be Reviewed on Appeal

Claims 1, 4-6, 8 and 9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2005/0123142 A1 to Freeman (hereinafter "Freeman") in view of U.S. Patent Application No. 2003/0028734 to March (hereinafter "March").

Claims 2, 3, and 7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Freeman and March as applied to claims 1 and 6 above, and further in view of US Patent Application No. 2003/0046544 to Roskind (hereinafter "Roskind").

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

7. Argument**A. Introduction**

The present invention is directed to preventing the unauthorized transfer of digital information from one device to another (p. 1, lns 5 – 7). It addresses the problem by providing for a secure transfer of digital information from a source device to a destination device (p. 1, lns 31 – 33). For example, music stored on a home device may be copied to a medium for playing in a car (p. 1, lns 11 -13).

A source device may contain a removable digital memory containing the digital information (p. 1, lns 33 – 35). An access card is used to facilitate the secure transfer of the digital information from the removable digital memory to an authorized destination device. For this reason, the access card is paired with the destination device. This “pairing” refers to a one-to-one correspondence that is established between the access card and the destination device, wherein the access card can only be used with the paired destination device (p. 6, lns 12 – 24).

The pairing of the access card with a destination device is done through the use of conditional access data stored on the access card and a user certificate data stored on the destination device. Initially, the access card authenticates that the destination device is authorized to receive the transferred digital information prior to the destination device receiving the digital information. This authorization is performed using conditional access data stored on the access card and user certificate data stored in the destination device (p. 5, lns 26 – 33).

Those having ordinary skill in the art will recognize that conditional access data and/or certificate data is designed to protect data that is provided to consumers which is

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

commonly used to prevent theft of cable TV services. The present invention discloses conditional access data and/or certificates which allow a user to access digitally protected data which the user has purchased. Such a system not only protects against copying by third parties, but also prevents unauthorized copying by the intended recipient of the data.

Once the access card authenticates the destination device, the destination device's public encryption key is written into a write once memory on the access card. This key is written into the write once memory in order to prevent pairing of the same access card with another destination device (p. 6, lns 12 - 24). This prevents the unauthorized access of the digital information on another destination device.

Encryption alone is not sufficient to prevent unauthorized access. The present invention uses a write once memory and pairing to ensure that the access card cannot be re-used by reinserting it into another destination device and overwriting the contents of the write once memory. The use of the both of these techniques prevents an owner of the source device from using the same access card to transfer information to another device other than the destination device.

Advantageously, a source device, an access card for enabling secure accession of digital information stored on a removable memory, a digital information destination device, and a method for securely transferring information from a source device to an external device are introduced which include novel features not shown in the cited references and that have already been pointed out to the Examiner. These features provide advantages over the prior art and dispense with prior art problems such as those described above with reference to the Applicant's specification.

It is respectfully asserted that independent Claims 1, 6, 8 and 9 are each patentably

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

distinct and non-obvious over the cited references in their own right. For example, the below-identified elements of independent Claims 1, 6, 8, and 9 are not shown in any of the cited references, either taken singly or in any combination. Moreover, these Claims are distinct from each other in that they are directed to different implementations and/or include different elements. Accordingly, each of independent Claims 1, 6, 8, and 9 represent separate features/implementations of the invention that are separately novel and non-obvious with respect to the prior art and to the other claims. As such, independent Claims 1, 6, 8, and 9 are separately patentable and are each presented for review in this appeal.

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

B. Whether Claims 1, 4-6, 8 and 9 are Unpatentable under 35 U.S.C. 103(a) over U.S. Patent Application No. 2005/0123142 A1 to Freeman (hereinafter "Freeman") in view of U.S. Patent Application No. 2003/0028734 (hereinafter "March").

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103. Section 2143.03 of the MPEP requires the "consideration" of every claim feature in an obviousness determination. To render a claim unpatentable, however, the Office must do more than merely "consider" each and every feature for this claim. Instead, the asserted combination of the patents must also teach or suggest each and every claim feature. *See In re Royka*, 490 F.2d 981 (CCPA 1974) (emphasis added) (to establish prima facie obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art). Indeed, as the Board of Patent Appeal and Interferences has recently confirmed, a proper obviousness determination requires that an Examiner make "a searching comparison of the claimed invention — including all its limitations — with the teaching of the prior art." *See In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original). "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

The Examiner has rejected Claims 1, 4-6, 8 and 9 under 35 U.S.C. § 103(a) as being unpatentable over Freeman in view of March.

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

1. Claim 1

Claim 1, in part, requires:

a memory for storing first conditional access data and at least one content encryption key;

a second port for receiving user certificate data and a first key of a key pair contained in a write once memory of an access card that has been paired with a destination device; and

a processor responsive to the user certificate data received on said second port for authenticating the received certificate data based on the first conditional access data stored in said memory, the processor, upon said authentication, encrypting information stored in said removable digital memory using the at least one content encryption key, to thereby provide encrypted information in said removable digital memory, the processor operable for encrypting said content encryption key using said first key received on said second port and outputting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device.

In the Office Action dated June 22, 2010 ("Office Action"), on page 6, the Office contended that Freeman does not teach that the access card has a write once memory and has been paired with a destination device. Because of this defect, the Office cited March and alleged that March discloses the above claimed feature. Applicant respectfully disagrees.

In the Office Action on page 3, the Examiner contends that "*March teaches a write-*

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

once memory [0037]. March teaches that data can only be written into the memory device by only the manufacturer of the device [0025]. Therefore, the manufacturer is paired with the memory device."

Although March discloses the use of write-once memory devices and describes the operation of the write-once memory devices with particular file systems, nowhere does March teach or suggest that the feature of an access card having a write-once memory and paired with a destination device. Again, the "pairing" as described in the specification refers to the fact that the destination device has been configured to work only with the paired access card in decrypting content keys from a given source device. An access card that has been paired with a particular destination device cannot be used to load content to another destination device, that is, it cannot be re-used with another destination device. Nowhere does March teach or suggest this feature.

The Office Action cites paragraph [0037] as teaching the write-once memory. Paragraph 0037 describes the disadvantage of a write-once memory that the memory cell cannot be erased once it is written into, and in fact, describes a method for **deleting data written to a write-once memory**. Therefore, this teaching is in direct opposition to the idea of using a write-once memory to pair the access card with a particular device since any pairing data in the write-once memory can be effectively deleted.

The Office Action cites paragraph [0025] as teaching the pairing of the access card with a destination device. In fact, March states in paragraph [0025]:

To ensure that the file system writes into only the smallest writeable unit of a memory device, it is preferred that the memory device comprise an indication of its smallest writeable unit (i.e., its line size) and provide this indication to the file system. The indication can be sent in response to a read command from the file system or can automatically be sent to the file system when the data storage system is

PATENT

Custmer No. 24498

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

powered-up or reset. The file system can receive this indication by sensing an electronic, mechanical, or optical feature of the memory device. For example, the indication can be provided in a register in the memory array or in a device identification code of the memory device. Further, the indication can be stored when the memory device is formatted or can be prewritten into the memory device by a manufacturer of the device. (emphasis added)

Thus, paragraph [0025] describes “an indication” that relates to the smallest writeable unit of the memory device. The indication is completely unrelated to user certificate data or a first key of a key pair as recited in claim 1. Rather, the indication is used by a file system to ensure that the file system writes into only the smallest writeable unit of the memory device. These are entirely different types of data, used for entirely different purposes.

Additionally, paragraph [0025] does not state that the “data can **only** be written into the memory device by **only** the manufacturer of the device” (emphasis added) as asserted by the Office Action. Rather, the paragraph clearly states that the indication can be stored when the memory device is formatted or by the manufacturer of the device. The fact that the indication can be written when the device is formatted suggests that other entities may write the data, and thus, the indication is not written by only the manufacturer of the device. Also, since the manufacturer is not the only entity that may write the indication into the memory device, the indication cannot serve to pair the memory device with the manufacturer. This is also clear from the function of the indication, which is to indicate an aspect of the memory device itself, not the manufacturer or any other entity that writes the indication into the memory device.

In view of the function of the indication, and the manner in which it is written to the memory device, it is not seen how such an indication can serve to pair the manufacturer with

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

the memory device in any way.

Independent claims 6, 8 and 9 include limitations directed to a pairing of the memory, or access, device with a destination device in a manner similar to that of claim 1, and thus, are believed to be patentably distinguishable over the cited combination for at least the same reasons as those discussed above with respect to claim 1.

Furthermore, one skilled in the art would not be motivated to combine the Freeman and March references, since the combination would not result in the claimed invention. Even if the references are combined as suggested by the Examiner, the combination would fail to disclose or suggest each and every limitation of the pending claims. As acknowledged by the Examiner, Freeman fails to provide an access card having a write once memory and pairing with a destination device. The cited March reference also fails to provide an access card having a write once memory and pairing with a destination device. In fact, March teaches away from such pairing since it describes a method for deleting data written to a write-once memory which is in direct opposition to the idea of using a write-once memory to pair the access card with a particular device. The combination would not result in any pairing data in the write-once memory since it can be effectively deleted. Therefore, a combination of the Freeman and March references would result in a system that does not pair an access card with a destination device thereby allowing unauthorized access to digital information by multiple destination devices. The combination does not teach or suggest "a second port for receiving user certificate data and a first key of a key pair contained in a write once memory of an access card that has been paired with a destination device" as recited in Claim 1.

Additionally, one skilled in the art would not be motivated to combine the Freeman and March references in the manner suggested by the examiner because they deal with

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

entirely different problems. Even if they are somehow combined together, one skilled in the art would realize that they would still fail to address the problem addressed in the claimed invention, that is preventing the unauthorized transfer of information from one device to another by providing for a transfer using an access card that is paired with a destination where the access card facilitates such pairing through the use of conditional access data.

Freeman is directed towards a system for changing encryption keys. In fact, Freeman simply makes no reference to conditional access data or conditional access certificates. The Examiner asserts that Freeman discloses these elements in its discussion of prior art key-change techniques (paragraph [0030]). However, one skilled in the art would recognize that the replacement of encryption keys is not conditional access data.

In the Office Action on page 3, the Examiner contends that "*Freeman discloses conditional access data. Freeman discloses that the certificate has a validity date [0028]. Since the certificate has a validity date (conditional time), Freeman discloses conditional access certificates.*" The certificates in Freeman recited in paragraph [0028] pertain to a public encryption key certificate and not to conditional access data.

March pertains to a system wherein a file system can dynamically respond to variability of memory cells in write once memory devices. March seeks to address the problem that while there are file systems designed for use with write one memory devices, these file systems may not be suitable for certain applications. However, March makes no reference to conditional access data or conditional access certificates.

Accordingly, one skilled in the art would not be motivated to combine the Freeman and March references in the manner suggested by the examiner because they deal with entirely different problems.

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

2. Claims 4-6, 8 and 9

It is respectfully pointed out that Claims 4-5 directly depend from independent Claim 1 and include all the elements of Claim 1. Therefore, Claims 4 – 5 are patentable for at least the reasons that they respectively depend from claim 1 and the rejection should be reversed.

Appellant's independent Claim 6, in part, requires:

"An access card for enabling secure accessing of digital information stored on a removable memory, the access card comprising:

a memory having stored therein a first conditional access certificate and a second conditional access certificate;

a write once memory;

means for authenticating first and second conditional access certificates with respective first and second certificate data stored on respective destination and source devices;

said write once memory, following authentication of said card with a destination device, being updated to store a public key of a public/private key pair stored in said destination device to thereby pair the access card with said destination device" (Emphasis added).

Appellant's independent Claim 8, in part, requires:

"memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device;

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

.....

an access card reader for reading an access card, where said access card includes authentication means and a write once memory which, prior to a first insertion in said destination device, includes at least a second Conditional Access Certificate and a first User Certificate and which, after said first insertion, includes at least said public portion of said private and public encryption keys thereby pairing the access card and the destination device and which, prior to a subsequent insertion in said destination device, is inserted into a source device and updated to include a content encoding key encrypted with said key encryption key, whereby said destination device, following said subsequent insertion of said access card, has the key encryption key and can decrypt said content encoding key and, using said content encoding key, decode said digital information encoded with said content encoding key” (Emphasis Added).

Appellant’s independent Claim 9, in part, requires:

receiving at the source device user certificate data from an access device that has been paired with a destination device and comparing the user certificate data with a first Conditional Access Certificate stored in memory of said source device for authenticating the certificate data” (Emphasis Added)

Claims 6, 8, and 9 are different from Claim 1, however the relative argument used above for Claim 1 may be applied to Claims 6, 8, and 9. Therefore, Appellant essentially

PATENT

Customer No. 24498

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

repeats the above arguments for Claim 1 and applies them to Claims 6, 8, and 9, pointing out why Freeman and March fail to teach or suggest the above claimed features. Thus, for at least the reasons discussed above for Claim 1, Claims 6, 8, and 9 are patentable over Freeman and March and the rejection should be reversed.

C. Whether Claims 2, 3, And 7 Are Unpatentable Under 35 U.S.C. § 103(a) Over Freeman In View of March As Applied to Claims 1 and 6 Above, And Further In View Of US Patent Application No. 2003/0046544 to Roskind (hereinafter "Roskind").

Claims 2, 3, and 7 depend from claims 1 and 6 and include all of the elements of their parent claims. Even assuming arguendo that Roskind discloses the subject matter as alleged, applicants submit that Roskind fails to cure the defect of Freeman and March as applied to independent claims 1 and 6. Therefore, it is believe that claims 2, 3, and 7 are patentably distinguishable over the suggested combination for at least the same reasons as those discussed above with respect to claims 1 and 6.

D. Conclusion

At least the above-identified limitations of the pending claims are not disclosed or suggested by the teachings of the cited references. Accordingly, it is respectfully requested that the Board reverse the rejections of Claim 1–9 under 35 U.S.C. § 103(a).

Please charge the amount of \$540.00, covering fee associated with the filing of the Appeal Brief, to Thomson Licensing Inc., Deposit Account No. 07-0832. In the event of any non-payment or improper payment of a required fee, the Commissioner is


PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

authorized to charge **Deposit Account No. 07-0832** as required to correct the error.

Respectfully submitted,

BY:


Paul Kiel, Attorney for Applicant
Registration No.: 40,677
Telephone No.: 609-734-6815

Date:

2/9/11

Thomson Licensing LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

8. CLAIMS APPENDIX

1. (Previously Presented) A device, comprising:

a removable digital memory including a port at which digital information stored on said removable digital memory can be accessed;

a memory for storing first conditional access data and at least one content encryption key;

a second port for receiving user certificate data and a first key of a key pair contained in a write once memory of an access card that has been paired with a destination device; and

a processor responsive to the user certificate data received on said second port for authenticating the received certificate data based on the first conditional access data stored in said memory, the processor, upon said authentication, encrypting information stored in said removable digital memory using the at least one content encryption key, to thereby provide encrypted information in said removable digital memory, the processor operable for encrypting said content encryption key using said first key received on said second port and outputting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device.

2. (Original) A device according to claim 1, further comprising means for establishing that said access card is not expired.

3. (Original) A device according to claim 2, wherein said means for establishing that said access card is not expired is performed by comparing the current time with a timestamp in said received user certificate data.

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

4. (Original) A device according to claim 1, wherein said first key is a public key of a public/private key pair.

5. (Original) A device according to claim 1, wherein said access card is inserted into a slot of said device.

6. (Previously Presented) An access card for enabling secure accessing of digital information stored on a removable memory, the access card comprising:

a memory having stored therein a first conditional access certificate and a second conditional access certificate;

a write once memory;

means for authenticating first and second conditional access certificates with respective first and second certificate data stored on respective destination and source devices;

said write once memory, following authentication of said card with a destination device, being updated to store a public key of a public/private key pair stored in said destination device to thereby pair the access card with said destination device; and

a processor operable for, upon authentication of said card with a source device, controlling transmission of said public key to said source device, wherein, in response thereto, said memory being updated to store encrypted data comprising a first key encrypted using said public key, said first key also being used to encrypt information on said removable memory at said source device, whereby communication of said encrypted data to said

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

destination device enables decryption of said data using said private key to recover said first key, to thereby decrypt encrypted information in said removable memory.

7. (Original) An access card according to claim 6, further comprising an electronic time stamp.

8. (Previously Presented) A digital information destination device comprising:

a digital information input port;

a digital information decoder coupled to said digital information input port for decoding digital information encoded with a content encoding key, when said content encoding key is available, to thereby produce unencoded digital information;

memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device;

a content encoding key decryptor for decrypting said content encoding key with a content encoding key encryption key;

an access card reader for reading an access card, where said access card includes authentication means and a write once memory which, prior to a first insertion in said destination device, includes at least a second Conditional Access Certificate and a first User Certificate and which, after said first insertion, includes at least said public portion of said private and public encryption keys thereby pairing the access card and the destination device and which, prior to a subsequent insertion in said destination device, is inserted into a source device and updated to include a content encoding key encrypted with said key encryption key, whereby said destination device, following said subsequent insertion of said access card,

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

has the key encryption key and can decrypt said content encoding key and, using said content encoding key, decode said digital information encoded with said content encoding key.

9. (Previously Presented) A method for securely transferring information from a source device to an external device, the source device having a removable digital memory containing information accessible to the source device, the information contained in said digital memory intended to be protected from unauthorized access, the method comprising:

receiving at the source device user certificate data from an access device that has been paired with a destination device and comparing the user certificate data with a first Conditional Access Certificate stored in memory of said source device for authenticating the certificate data;

accessing, by said source device, said information stored in said removable digital memory and encrypting said information stored in said removable digital memory using at least one content encryption key stored in said source device, upon authentication of said certificate data;

receiving at the source device a public key from a write once memory of the access device and encrypting said at least one content encryption key using said public key; and

transmitting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device communicable with said access device.

10. (Previously Presented) A method for securely porting digital information from a source device to a destination device comprising:

PATENT

Customer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

providing a source device having a removable digital memory and including a first Conditional Access Certificate;

providing a destination device having a second stored User Certificate and also including mutually corresponding private and public encryption keys associated with said destination device;

providing an access card capable of use with both said source device and said destination device, said access card including a second Conditional Access Certificate and a first User Certificate stored therein;

placing said access card in said access card port of said destination device a first time;

after said placing of said access card in said destination device a first time, accessing said second User Certificate from said destination device, and, within said access card, authenticating said second User Certificate from said destination device with said second Conditional Access Certificate to determine if said public encryption key should be read from said destination device and stored in said access card;

if said public encryption key of said destination device should be written to said access card, writing said public encryption key from said destination device to said access card;

removing said access card from said destination device after said writing of said public encryption key;

inserting said access card into said source device, and authenticating said first User Certificate with said first Conditional Access Certificate to determine if said access card is valid;

if said access card is deemed to be valid by said source device, copying said public

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

encryption key from said access card to said source device;

at said source device, encrypting at least some of said digital information in said digital memory using at least one content encryption key to produce encrypted information, using said public encryption key from said destination device to encrypt said content encryption key to thereby generate at least one encrypted content encryption key, and storing said at least one encrypted content encryption key in said access card;

connecting said port of said digital memory to said digital information port of said destination device;

placing said access card in said access card port of said destination device a second time;

after said step of placing said access card in said access card port of said destination device a second time, copying said at least one encrypted content encryption key from said access card to said destination device, and decrypting said encrypted content encryption key using the private key; and

at said destination device, receiving said encrypted information from said digital memory, and using said content encryption key to decrypt said encrypted information.

11. (Original) A method according to claim 10, further comprising the step of establishing that said access card is not expired.

12. (Original) A method according to claim 11, wherein said step of establishing that said access card is not expired is performed by comparing the current time with a timestamp in said User Certificate.

PATENT

Custmer No. 24498
Attorney Docket No. PU030342
Final Office Action Date: 6/22/10
Advisory Action Date: 10/19/10

13. (Previously Presented) An access card, said access card comprising:

a memory having at various times at least first, second, and third states;

authenticating means;

said memory comprising, in said first state, a second Conditional Access Certificate and a first User Certificate stored therein;

said memory, in said second state, following a first insertion of said card and first authentication, where said first insertion of said card is into an access card port of a digital information destination device including a digital information port which is capable of receiving said digital information, a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device, and said first authentication is performed by said authenticating means authenticating said second User Certificate from said destination device with said second Conditional Access Certificate, comprising said public encryption key from said destination device;

said memory, in said third state, following a second insertion of said card and second authentication, where said second insertion of said card is into an access card port of a digital information source device including a removable digital memory containing digital information and a further memory containing a first Conditional Access Certificate and at least one content encryption key, and also following authentication of said first User Certificate stored in said memory of said access card with said first Conditional Access Certificate stored in said source device to establish validity of said access card to said source device, comprising said at least one content encryption key encrypted with said public encryption key.

PATENT

Customer No. 24498

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

9. **RELATED EVIDENCE APPENDIX**

None.

PATENT

Customer No. 24498

Attorney Docket No. PU030342

Final Office Action Date: 6/22/10

Advisory Action Date: 10/19/10

10. RELATED PROCEEDINGS APPENDIX

None